EXHIBIT G

WHAT IA WELL AND RESIDENCE OF THE PROPERTY OF

RealSecure 1.0 for Windows NT

Monitor your network and protect it from malicious attacks



Attacks on networks connected to the Internet are rampant and getting worse. People

are continually discovering new ways to break into or disable Windows NT. You are justified in protecting your network, but you need tools to do the job. One gem of a network protection tool is RealSecure 1.0 for Windows NT, from Internet Security Systems (ISS).

You might think your network is pro-

tected adequately, but how do you know for sure? Do you know when someone is trying to break in or attack a network service? Maybe you monitor the attack logs that your security systems produce. Although monitoring system logs is a great practice, it doesn't stop

attacks; it simply informs you that an intrusion occurred.

Not all security systems can recognize all forms of attacks. Frequently, you have to program a security system with information about an attack type before it can prevent or detect it. The security system you bought last year might not adequately handle this year's attack methods. The solution is to keep your security systems up-to-date, a timeconsuming but worthwhile effort.

Between updates to your security systems, RealSecure, a realtime network attack recognition system, can help you monitor network security. RealSecure looks at network traffic at the packet level (much like a network sniffer) and uses its built-in attack recognition logic and definable filtering rules to determine whether the packets are potentially malicious. (RealSecure can recognize more than 200 different system attacks.) Filter rules

define the action to take when

by killing the affected network sessions. Powerful stuff, to say the least.



Let's take a quick look at RealSecure's components to see how they interact. RealSecure installs as an application console, a network service (which ISS calls an engine), and a custom packet driver that you load with your other network protocols.

The RealSecure engine reads the

RealSecure detects an attack. When it finds suspicious packets, RealSecure can record the date, time, source; and target of the event; record the event's content for session playback; notify administrators of the attack; or terminate the attack

SCREEN 1: Displaying the filter logic of the Maxi-

mum Coverage

template

32 . A	Provid Marrie	Prior	holly Client	Actions	SOURCE ACM	Destination	Proto	SOLFEE	(restleation)
12.75	POP3	Low	Þ.	1	Any	Alty	#TC	Ahy	(POP3
E777	PORTMAPE	ikow :	P	1	Any	An	170	:Ary	Portmop
54.4	N a UD	Low	- P	1	AW	Amy	1C	Any	,NMTP
11.55	MAP2	Low	P	Î	My	Any	iIÇ	Arry	MAP
083	RC	Low	P		ACH	Any	1C	Arry	RC serv
1 1 1	DEM	Low	P	Į.	MY	Any	TC	Any	,idert :
2:YG	HFS	Low	₽	1	Arry	Arry	IC	Any	9FS
7-67	SATAN	Low	7	9 7	Any	Arry	ITC	Arry	TCP-MUX
42.2万	EO4O	Low	₽ .	1	Arry	Alty	(TC	Arry	Echo
5	CHARGEN	Low	₽.	6	:Atry	Arry	!rc	AIN	Chergen
B\$\0	DNS	Low	. 7		AN	Arry	;UD	Am	DNS
172.76	TETP	Low	P		'Ary	Any	JUD	ATY	ETP.
6,45	RMHO	LOW	1 7	7	'ልጥ	Any)ÚD	Alty	Yrtx:
IDEX	KERDEROS	Low	7.	1	Arr	Any	iuo	Arry	kerberos :
31 23		TIVE	CHARLES IN	CVP. R	DESCRIPTION.	ing batter to			
F 30:3	सर्वेद्याप्टरकर -	45.543.5	12	525	uceunii (s	100 100 100		Jan Bra	CD-2015
	WC37/210	Address	7				-		WITTE S



packets as they arrive at the network interface from the packet driver. The engine compares the packets to established filtering rules. If the engine finds a packet that matches a rule, the engine's attack recognition logic parses the packet information. If the logic detects an attack, the engine takes an appropriate action as defined in the filtering rules. The engine also sends all packets that match the filters to the console for logging, reporting, session playback, or review.

Installation and Configuration

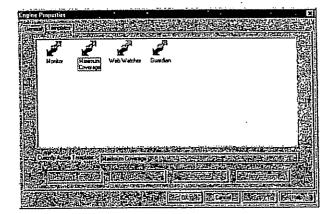
Installing the software is quick and painless. You need to install the software on each segment that you want to monitor. You can load a packet driver and engine on an NT system residing on each remote segment and then load a single centralized console on an NT system that collects data from the other RealSecure engines. If your network is simple (i.e., it uses only one network segment), you can load one copy of RealSecure on any NT box to monitor your entire LAN. Each console uses an authenticated and encrypted system-tosystem session to talk with a remote engine. This process prevents any tampering with your RealSecure monitoring system's network traffic.

After you've installed RealSecure on each system, you fire each one up and configure it. Configuring RealSecure means defining which attacks or suspicious activity you'd like to watch out for (called filtering) and what to do about a particular event when RealSecure detects it. For example, if your network security policies disallow all inbound Telnet sessions and you've adjusted your firewall to prevent them, you could configure RealSecure to watch for

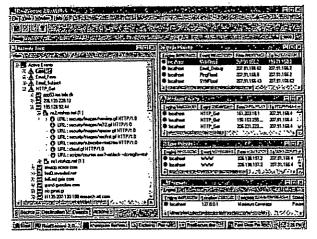
➤ SCREEN 2: Viewing the engine's attack signatures

ناخير	Decide Expe	Price by to	betty Chi	CACHE	Printing Description 15 57	۰
P	IDENT_USER	'Medun	(F)	·	kiert ther Decode	
P	FOUPLEATE	High	P	1	Choca for duplicate P's.	
Ø.	PFRAG	14gh	. 6	7	Check for P Fragrents with offset Exestin	
ק	PHALESCAN	iHigh	<u> </u>	0	Check for people halfscarring your network	
F	PHOFEDOD	High	LE.	70	:Prog flooding threshold in packets/second	
P	POP PASSWORD	Modken	1 17		Decrete POP Pastword	
₽.	POP_LESER	Medium		i	Decode POP Usernene	
7	RLOGN	'Medum	<u> </u>	1	'Decode Riogin Sasakn	
P	TRECORN FROOT	High	<u></u>	1	'Riogen-Irroct Cheach	3
7	RSH	- March an	P	<u> </u>	Decade RS4 Sessions	Š
F	ISCURCEROUTE	High	P	i/	,	ď
P	SYMPLOOD	High		:/ 0	Check for SYN Flood	ŗ
P	LOPEOME	High	<u> </u>	!/ B	Check for LDP Bords	2
	1		1	1	<u> </u>	÷
e k:	THE PERSON	スカン かんしょう かんしょう	4-4-18-		ে ্ নিজেনক	ı.
22121	BREAK STEELS	S 64 1 1 0 1	Section.	李利尼是		

Screen 3: Selecting a filtering profile



SCREEN 4: Viewing RealSecure's console interface



inbound Telnet connections. If an intruder defeats your firewall and launches a Telnet session, RealSecure can detect the session, shut it down immediately, and record a detailed log of what occurred during the session.

RealSecure can recognize hundreds of potential attack scenarios. Screen 1 shows some predefined filter logic of the Maximum Coverage template; Screen 2 shows some attack signatures used for detection in the attack recognition portion of the engine. You can use the built-in templates or define your own.

After you configure the software, you assign your chosen filter profiles to each engine on your network. To assign filters to an engine, right-click an engine listed in the Engine window, choose Properties, select a filtering profile from the choices (as you see in Screen 3), and click Apply to Engine. The engines start up using the specified filters and begin acting as your network watchdogs. You can manage all engines, local and remote, from one centralized console, which simplifies management in a distributed environment.

CONTROL OF TAXABLE PRODUCTION OF THE PRODUCTION OF THE PRODUCTION OF THE PROPERTY OF THE PROPE

RealSecure in Action

RealSecure's console is the central place where you review the captured suspicious network activity. As you see in Screen 4, the interface has five windows. In the left window, you can see a hierarchical view of the source address, the destination address, events, or actions taken on those events. This window's NT Explorer-style tree view provides an easy way to drill down to the capture information. The three top windows on the right (High Priority, Medium Priority, and Low Priority) display each type of captured event according to its definable priority level. The Engine window identifies the location of the engine and the template being used for monitoring.

Screen 5 shows a maximized view of the Medium Priority event window. As you can see. RealSecure has captured many events that I defined in the filters as being of medium concern to me. These events are mainly HTTP_Get requests, the usual request a Web browser uses to retrieve a Web page. RealSecure captured the name of the engine reporting the event, the Web Get request, the user's IP address (source address), the destination address (my Web servers' addresses), the URL used to retrieve the document or file, and the time and date Ordinarily, you don't want to monitor every user retrieving simple Web pages from your server, but I do because my Web site has encountered suspicious activity in the past. Tracking all access might help me catch an intruder red-handed.

High-priority events are the most interesting. During my test, I launched many attacks (ping floods, SYN floods, IP spoofs, User Datagram Protocol bombs, and several other common intrusion attacks) on my systems to see how RealSecure would react (as shown in Screen 6). As I expected, RealSecure immediately detected my attacks, collected information about them for my review, and shut them down.

Another nice feature of RealSecure is its ability to capture and replay entire network sessions. For example, you can define a filter to track and capture

LAB REPORTS · RealSecure 1.0

attempts to Telnet into your router or other systems. Later, you can replay the session to see what the intruder was doing. You can use these captured sessions as evidence against the would-be intruder if you prosecute. Really slick and greatly needed.

The software is robust and easy to use, and it has plenty of useful features. A report generator produces formatted reports. And the ISS support team does a fantastic job of answering your questions.

The second major release of Real-Secure will contain new functionality such as automatic attack logic updates over the Internet and the ability to push RealSecure out to remote servers without special software such as Microsoft's Systems Management Server (SMS). RealSecure runs on NT and on a variety of UNIX operating systems, and the program can detect attacks against any operating system using TCP/IP, not just NT.

I want to point out that someone could misuse RealSecure's power internally to launch attacks against your network. For instance, just as you can use RealSecure or some other software to prevent users from surfing to certain Web sites, disgruntled employees could use RealSecure to attack your network or wreak havoc on connecting net-

MARKET BUTTON	THE TOUR DO	Part Clared Co.	一十二十二十二十二十二十二十二十二十二十二十二十二十二十二十二十二十二十二十二	● できたが、いですい。までは、まかられることをからは、	Date からななべかからない
DOM: NO	HITP Get	1\$1,223,16,1	207.31.168.6	URL - CLDUD GR HTTP/A.0	F4AJ111254491997
location.	HETP Our	1241数压。	207.31.165.4	URL-security/mages/five-educationaryage	F#A#11125F#F1932
Ecarem	HIII Ger	XE XX 222	207.51.164.4	UPE - PROCEEDINGS OF THE STATE	F4 AU 11 12 St 42 19275
bestud	H) tr Gu	141.2 17.3	227,51.162.4	UPE - mounty/magnet/from adultance git.	FAART 1256 67 1927
to a red	HIIP Ge	192167.6111	207.91.118.4	UPL - recurringer/hy-edutatec.pl	Fe A # 13 12:54.47 1957)
Total Seed	HITT DA	1412173	207.31.166.2	CPIL - ecopy/recay pags HTTP/TLD	F4A41E1254 44 1997
local-and	HITP. DM	はというない。	207.51,102.4	UPIL + scripts/hetop.org/HTTP/ILB	F# A.# 11 12:54 45 1317)
beatest	HTTP_Get	157,253,163	27.91,18.4	URL - receiptages/for each tenance.	Fri Auf 11 12:54 44 1957s
Security and	HITP OH	112 127,6111	207.91,106.4	UFIL - ecripto/betts sep HTTP/5.0	Fe A 6 11 12:54 43 19175
COST WE	SULS THE	157,753,163	20731,1564	UFIL scripts/herp arp I/TTP/1.9	76 Ag 11 1254 42 1957)
to all total	HTSP Cal	205 177 203 20	207.91,166.4	UPL-security/inspec/i-s-ect/re-ect/	NAMES 1354 42 1999
tocareet	HTTP_GM	152 174 22 23	207.51.135.4	URL HTTP/LD	Fr A # 11 1259 00 1977
burben	IT EF	225 221 222	207.57.146.2	UPL + roughs/courser swn?-sublantsdo	F4 A £ 11 12:51:30 (997)
bullete.	HETTP_E#	XX 231 221	207.93.16%, 4	LIFEL a recruite/beagain/reclinit pd HTTP	Fei Aut 81 13:50 20 1997)
bullent	KEIT Det	3E 271.227	37.51.114.4	LERL - moultainmounte(12 pt HTTP/T-B	Féaget 12:54:37 1957;
beares	H777 Get	202 271 222	207.51.166.4	LIFE - NACUSAN AND SOUTH LESS AND SO	Fe Ad 11 13 54 37 1257)
locahost	KITP_Get	275 271 222	対別 1 1 英 4	URL receipted position acres by H.	FeAUSE 13 94 37 1937)
tacamen	HITP Ge	25 271 272	307.91.166.4	LIFE, - excuse/respectations of HTTP	FrAJ 11 13 54 37 1907)
) besitest	HITP GE	298.1 L227.71	207.91.16E.4	URL construences for advisorance.	Fi 3211 133137 (303)
bc.ercel	HTT Ga	130 225 73 17	207.57, 108.4	1FQ - recurs/requires and/street/1.	Fe AJ 11 13:54:37 1997)
> bonton	111 17 June	35 130 117.2	207.31.158.4	URL reside \$11770.0	FFAX11 13:5436 19979
استراط ا	H23) _ Bas	13857872	207,51,168.4	UTIL - records/fragra. Res-palc/records.	F4AJ311254361997
المجاورها ا	Kill Gar	100元15	207.91.158.4	URL closed of HTTP/LD	FIANT 1254 M 1957
D becarbone	HTTP Det	204.231.232	207.51.112.4	UPL - reculp/inspec/sorring at HTTP	Fi & 11 125435 1907)
local set	1117 Jim	304 221 222	207.31.116.4	UPA - consump Annual Assessment of HTT	Fri Ad 11 12 54 35 1957)
licatus .	HTTP Get	25 ZR 272	27.21.166.4	UPR, worshipmen/planting of \$17_	FEAR11 13 54 25 1307)
focurent	14737_Gas	2012/21/10	337.51.165.4	U.S. HOLLING MARRIED SCHOOL SELL	FLAG11 1254.36 1973
li locations	HTTP Gat	274 271 272	207 St. 152 8	UPL-seculations for address X.	(VAJ S 1354.251927)
₱ bunhert	HITH ON	208 1B 227.71	207,57,186 C	LIFE, - accepta/indup and HTTF/1.8	Fe3411 1354 251807
D brokens	NETT De	1905167.2	267.91.116.7	URL HOUSE/Beds and HTTP/1.0	Fax 111 1254 34 1977
I BANCO DI VIS	recolution and	Cracia dise	AND DESCRIPTION OF THE PARTY OF	Promitive survivation in the same below.	روي ومنبوختيمة منسوسيسين

≼ SCREEN 5:

Displaying a Medium Security events window

| Company | Comp

SCREEN 6: Viewing active attacks

works. Treat the tool like any other sensitive information or equipment: Limit access so that only trusted operators can get to the RealSecure consoles. In the next version of RealSecure, ISS will add a feature that lets RealSecure detect other copies of RealSecure on the network; this feature will help control internal misuse of the software.

I'm impressed with this new product, and I feel much more secure about my LAN environment now that I have it installed and running. RealSecure is a must-have package for any serious network environment, especially if you're connected to untrusted networks such as the Internet.

ABOUT THE AUTHOR

Mark Joseph Edwards is a writer and network engineer with more than 16 years of experience in network engineering and communications. He is the news and UPDATE editor for Windows NT Magazine, founder of Netropolis Technology Group (NTg), and author of Internet Security with Windows NT, forthcoming from Duke Press. You can reach him at

ISS_02125874



Internet Security Systems, Inc. (ISS)

41 Perimeter Center East

Atlanta, GA 30346

Phone: 770-395-0150

Phone: 800-776-2362

770-395-1972 Fax:

Email: iss@iss.net www.iss.net